XXII IPSA World Congress of Political Science, Madrid, 8-12 July 2012

Section Title: **Immigration and asylum policy**

Panel: **Rethinking Borders and Boundaries**

Author: **Artur Gruszczak, Jagiellonian University, Krakow, Poland**

Title: **Do smart borders make good fences? The EU's experience in an integrated border management**

Introduction

The European Union (EU), despite recent legal and institutional changes, has kept its hybrid nature. This is due to the fact that the European Union is a special kind of epistemic/ organizational/regulatory community "cursed" by hybridized relationship between actors and structures at transnational, supranational and intergovernmental levels, between external and internal dimensions of EU politics, between modern nation-state and postmodern cosmopolitan democracy, which "contaminate" the structures of power, authority, accountability and territoriality.

Hybridness seemed to be the strength of the EU, giving her immunity from crises of identity and legitimacy, favoring changes and reforms, stimulating spillover of integration. The current crisis of the EU has reduced positive effects of hybridization and highlighted disadvantages and weaknesses with regard to the integration process. Nevertheless, hybrid features still prevail in an area of greatest sensitivity and importance for EU institutions as well as the Member States: that of security. EU security area is still divided into internal (Freedom, Security and Justice) and external (Common Security and Defence) fields; law enforcement, judicial and military cooperation; European security strategy and EU internal security strategy; the core and peripheria (opt-out countries); Schengen and non-Schengen countries. Despite numerous attempts at working out a comprehensive approach to EU security, differentiation and hybridness determine activities undertaken by EU institutions, agencies and Member States.

The European Union as an ever closer union of more integrated nation-states and societies has brought about important achievements: the Schengen area of free movement of persons, common asylum policy, cooperation in the field of migration and borders. All of them originated in a postomodern approach to territory and borders as state institutions. No control at internal borders within the Schengen zone, externalization of Justice and Home Affairs cooperation based on partnership and close links to neighbour countries, local border traffic agreements with non-EU states – these were clear examples of political deterritorialization of EU policy.

Yet the European Union has failed to create secure and stable environment as transnational threats have been rising and the EU has been under constant pressure from transnational actors: terrorist groups, drug smugglers, traffickers in human beings, illegal migration networks. Hybridity of borders – as walls and points of access as well as gates of passage to the better world[1] - was brutally tested during the 2011 "Arab spring" and a massive, though short-term, flow of North African refugees to the EU. Following the upheavals in North Africa and the Franco-Italian anti-Schengen dispute, The European Council in June 2011 adopted conclusions calling for an enhanced cooperation between border control agencies from the Member States, effective surveillance of the EU's external borders and application of new technologies. Borders were to be transformed into security policy areas where high-tech tools, professional management skills and extensive normative measures should be strictly applied.

The 2011 border crisis was a catalyst of reinforced control and more efficient management of external borders of the EU. However, trends towards the introduction of new measures, tools and mechanisms of protection, control and surveillance of borders were identified much earlier. Highlighting threats and risks coming from criminal activities developed by organized criminal groups, gangs and "mafias" was the traditional element of securitization of EU external borders. The need to introduce strict protection measures, develop and modernize technical and organizational means of control and surveillance was legitimized by preventive and protective role of state authorities (police, gendarmerie, border guards) against growing irregular migration as well as expansive criminal gangs.

[1] H. Cunningham, Nations Rebound?: Crossing Borders in a Gated Globe, *Identities: Global Studies in Culture and Power*, 2004, 11 (3), p. 333.

The European Union since 2006 has been decisively pushing the Member States for introducing, developing and reinforcing elements of an integrated border management system, especially by implementing and enhancing high-tech devices and solutions typical for the concept of 'smart borders', or 'e-borders'. The making of digital borders by the EU's institutions and the member states reflected to some extent the logic of exclusion in the field of migration and asylum policies yet at the same time stemmed from the need of administrative efforts at securitization of the public sphere through digitalization of personal identity management.[2] The historical evolution of the Schengen area has proved that compensatory measures were increasingly tied to technological solutions and electronic devices applied to strengthen protection and control of external borders.[3]

This paper seeks to verify to what extent elements of 'smart borders' meet effectively expectations formulated by governments and citizens of EU Member States with regard to an effective protection of internal security and efficient management of external borders of the EU. Therefore, the model of an EU integrated border management will be analyzed in the context of "digitalization" and impact of "smart" technologies. The Commission's communication on "smart borders" of October 2011 will be assessed in the context of technology-driven systems of data collection, storage and comparison with regard to third-country nationals coming to the EU. The thesis developed throughout this paper is that the concept of "smart borders" as part of EU integrated border management system falls within what Hooper defined as borderwork, i.e. a mechanism of physical and "virtual" (digital) differentiation leading to boundary maintenance and cleavage reinforcement.

The paper is divided into three parts. The first part gives a picture of the European Union as "security enclave" possessing major features characteristic for "gated communities". The next part provides a detailed evaluation of the EU's integrated border management system. Final part contains an analysis of the latest communication from the European Commission on "smart borders".

---

[2] See D. Broeders, *Breaking Down Anonymity. Digital Surveillance of Irregular Migrants in Germany and the Netherlands*, Amsterdam, Amsterdam University Press, 2009, pp. 197-99; D. Broders, The New Digital Borders of Europe. EU Databases and the Surveillance of Irregular Migrants, *International Sociology,* 2007, 22 (1), pp. 87-89.

[3] See D. Bigo, *Polices en reseaux: l'experience europeenne*, Paris, Presses de Sciences Po, 1996; D. Bigo and E. Guild (eds.), *Controlling Frontiers. Free movement into and within Europe*, Aldershot, Ashgate, 2005; E. Brouwer, *Digital Borders and Real Rights. Effective Remedies for Third-Country Nationals in the Schengen Information System*, Leiden – Boston, Martinus Nijhoff Publishers, 2008.

The European Union as a security enclave

In 1995 seven of the EU Member States abolished their internal borders and allowed for a free movement of their citizens and legal third-country nationals across their territories. The emergence and subsequent extension of the so-called Schengen area was a great leap forward since persons staying within this area could travel freely without border controls, yet at the same moment the external borders were transformed into dense networks of surveillance and control taking advantage of new advanced technologies of personal identity management, early warning and threat prevention regarding cross-border human and material flows.

At the time of emergence of the Schengen area transnational processes changed traditional perception and understanding of security. Globalization, deterritorialization and networking had a profound impact on European internal security. They allowed not only for circulation of ideas, international economic exchange, human mobility and development of interpersonal relations in the global scale, but also made room for proliferation of transborder threats, pathologies and various forms of criminal activities. Paradoxically enough, factors facilitating transnational cooperation, economic integration and free movement of people prompted the emergence of new policies and measures seeking to restrict liberties and strengthen the resilience for threats and hazards. Securitization of migration policies, restrictive asylum policy, strict EU visa regime and proactive border control and management gave altogether grounds for a new approach towards free movement of persons and flanking security measures. A shift from liberal stance to a more restrictive attitude towards EU citizens' (personal data protection) and migrants' rights, territorial dimension of security undertakings and massive impact of surveillance techniques and technologies made the Union resemble a "gated community" or "defended neighbourhood" underlying thus the "enclave-like" feature of the European Union in terms of global migration, cross-border flows and cultural shifts.

In its "classical" meaning of the 1990s, the EU as a security enclave comprised a complex set of political activities undertaken by the member states, assisted by EU institutions, bodies and agencies, to secure high level of safety to EU citizens and legal aliens

as well as to respect civil liberties and fundamental rights. EU internal security governance was strongly influenced by "schengenization" of normative framework for internal security cooperation.[4] The reinforcement of external borders, harmonization of methods, tools and procedures of border control, common visa policy and the fight against illegal migration and trafficking in human beings were glaring examples of protective measures adopted by the EU member states. In the face of new challenges and threats that emerged at the beginning of the present decade, those measures resulted to have limited efficiency and scope. Following the tragic events of the 9/11, the member states in cooperation with the Commission engaged themselves in the project of an integrated border management system consisting of multi-level coordinated mechanisms of protection and control of external frontiers of the EU. It was intended to demonstrate that the EU as security enclave had been constructed in a single territorial entity consisting of complex, multitiered, geographically overlapping structures embedded into multilayered security regimes.

What is symptomatic for the EU as "protection space"[5] is the stress on physical identification of persons crossing the external borders or residing on the territory of Member States, the technologically biased management of identity of third-country nationals through high-tech systems of border surveillance, perimeter control, automated targeting and risk-profiling.[6] Application of protective devices, security technologies and remote sensor surveillance is aimed at establishment of "defensible space".[7] EU projects that have been unfolding recently (SIS II, VIS, Eurodac, entry/exit) are based on highly advanced communication and control technologies and resolutely introduced biometrics. This relatively new technique of personal identification and authentication is particularly important in the context of security management, allowing for advanced personalization of administrative measures concerning both EU citizens (ID cards, passports, mobile telephony) and aliens (visa, asylum application, border control). This is an effective tool against illegal migration (like Eurodac fingerprint data system), but also an instrument facilitating certain procedures related to freedom of movement (like IRIS system of control on selected British

[4] A. Gruszczak, Networked Security Governance: Reflections on the E.U.'s Counterterrorism Approach, *Journal of Global Change and Governance,* 2008, 1 (3), pp. 4-5.

[5] See M. Rhinard, M. Ekengren, A. Boin, The European Union's Emerging Protection Space: Next Steps for Research and Practice, *European Integration*, 2006, 28 (5), pp. 514–17.

[6] B. Hayes, *NeoConOpticon. The EU Security-Industrial Complex*, Amsterdam 2009, p. 34; A. Mattelart, *La globalisation de la surveillance. Aux origines de l'ordre sécuritaire*. Paris 2007, pp. 197-209.

[7] E.F. Harshman, J.E. Fisher, W.B. Gilliespie, J.F. Gilsinan, F.C. Yeager, *Gated Communities In Cyberspace*, http://www.scu.edu/ethics/publications/iie/v9n3/gated.html, (accessed on 20.03.2008).

airports).[8] This is at the same time a powerful tool allowing for construction of a sophisticated system of individual control and surveillance in order to prevent and counter major threats to internal security like terrorism or WMD proliferation. Hitherto projects carried out by EU countries are concentrated on external border security measures, involving a specific "biopolitical technology"[9] (biometric or machine-readable passports, biometric visas, fingerprint and body scanners) as well as high-tech means of border control (satellite surveillance, infrared monitoring, electronic fences and even spyplanes[10]).

Even if technological advances could be translated into new methods and tools of securitization, cooperation of police and border guards is equally important. As Bigo and Carrera maintained, the "blinded belief in the use of technology as a way to solve political problems […] creates more problems and insecurity than it helps to tackle the initial problem itself".[11] The cooperation between law enforcement agencies, especially national police forces supported by Europol-coordinated information management units have to be coupled with high-tech surveillance and control facilities. Nodes of police cooperation, taking advantage of intelligence-led policing, electronic surveillance, biometric authentication, could best secure national security interests, international binding security arrangements and individual needs, constraining from an overwhelming impact on the public sphere and from permeating social interactions and individual behaviour. This is due to the fact that cooperation in the area of the EU's internal security covers a vast terrain where multiple actors on transnational, national and sub-national levels enter in complex interactions mapping out or bringing about diverse models of security and agendas for public order.

The need to establish stronger and more politically-oriented bases for internal security policies as well as the pressure to set them into motion as quick as possible contributed to the employment of strategic thinking into conceptual works and policy-making. In the aftermaths of the 2004 Madrid terrorist attack, unlike post-9/11 developments, the need for concerted action was evident on the level of the European

---

[8] See Iris Recognition Immigration System, http://www.iris.org.uk and e-Borders Programme, http://www.ukba.homeoffice.gov.uk/travellingtotheuk/Enteringtheuk/usingiris/ [accessed on 11April 2009].

[9] J. Huysmans, A Foucaultian view on spill-over: freedom and security in the EU, *Journal of International Relations and Development*, 2004, 7 (3), p. 308.

[10] B. Hayes, *Arming Big Brother. The EU's security research programme*, Amsterdam 2006.

[11] D. Bigo and S. Carrera, From New York to Madrid: Technology as the Ultra-Solution to the Permanent State of Fear and Emergency in the EU, CEPS, Brussels, April 2004; http://www.ceps.be/Article.php?article_id=314 (accessed on 25.05.2004).

Union. Moreover, given political and operational reasons as well as domestic circumstances in certain Member States, EU cooperation had to take into account common actions and strategies worked out by the institutions and bodies of the Union in its legal and institutional framework. The whole package of interlocking strategies of internal security management was based on the principles of diminishing threats (both internal and external) and reducing vulnerability. Some of those strategies have been outlined in general terms (the 2003 European Security Strategy, the 2010 Internal Security Strategy); others were designed specifically to tackle the challenges of cooperation in the area of freedom, security and justice (the 2005 Strategy for the External Dimension of Justice and Home Affairs; the 2004 EU Drugs Strategy 2005-2012; the 2005 strategy for combating radicalization and recruitment into terrorism); still others kept a horizontal position (the 2005 Counter-Terrorism Strategy).

Nearly all of the above-mentioned strategies stemmed from an optimistic supposition that societal sphere of the EU is sufficiently strong to neutralize and absorb dysfunctional undertakings planned or committed by enemies of freedom and democracy through mechanisms of inclusiveness inherent in EU politics, deep-rooted in democratic and liberal tradition of an EU supranational community.[12] However, it is often stressed that indigenous factors of instability and jeopardy are closely interlinked with external sources of threats and menaces, often strongly motivated by religious or cultural reasons. This is particularly important in the present era of asymmetric threats and conflicts where danger may come suddenly and provoke an immediate outburst of panic and destabilization. The 2005 Strategy for the External Dimension of Justice and Home Affairs was based on a thesis that the emergence and reinforcement of an area of freedom, security and justice in the EU can by successful only when the external political and social environment, particularly in adjacent and neighbouring areas and regions, will offer favourable conditions in terms of partnership, cooperation and threat reduction. Nonetheless, the EU should be more proactive in countering threats and challenges coming from outside, pursuing in close cooperation with third countries both actions to tackle irregular flows and cross-border crime and this should include efforts to strengthen border controls, improve travel

[12] See C. Beyer, The European Union as a Security Policy Actor: The Case of Counterterrorism, *European Foreign Affairs Review*, 2008, 13 (3), pp. 302–03.

document security and combat people smuggling and trafficking.[13]

The latest strategic blueprint put forward by the Council in February 2010 pointed out that internal security had to be understood as a wide and comprehensive concept which straddles multiple sectors in order to address major threats through an integrated action in the area of law enforcement and judicial cooperation, border management and civil protection. The Internal Security Strategy for the EU put a special emphasis on new technologies playing a key role in border management. According to the Council of the EU, technologies "may make it easier for citizens to cross quickly at external-border posts through automated systems, advance registration, frequent-traveller schemes, etc. They improve security by allowing for the necessary controls to be put in place so that borders are not crossed by people or goods which pose a risk to the Union.[14]

The European Union as security enclave has been step by step heading towards "virtual fencing"[15] being a networked structure of high-tech solutions and devices built at external borders, connected to external "posts" (consulates for instance) and backed by inner sophisticated data bases and search engines collecting, sharing and processing information concerning third-country "elements" flowing into the EU's territory. Integrating those technologically-driven control and surveillance devices with strategy-oriented policy tools of border management quickly resulted a priority for the Member States as well as EU institutions and agencies in charge of internal security of the Union.

EU Integrated Border Management - the state of play

Migration has long been an important phenomenon for European societies, economies and – last but not least - identity. Regardless of massive internal migration flows in the aftermath of the EU's "Eastern enlargement", the immigration from third countries

[13] A Strategy for the External Dimension of JHA : Global Freedom, Security and Justice, doc. 14366/3/05 REV 3 LIMITE, Brussels, 30 November 2005.
[14] Draft Internal Security Strategy for the European Union: "Towards a European Security Model", Council of the European Union, doc. 5842/2/10 REV 2, Brussels, 23 February 2010.
[15] See: P. Andreas, Redrawing the Line. Borders and Security in the Twenty-First Century, *International Security*, 2003, 28 (2), p. 92.

almost equaled the amount of intra-EU migration (in the period 2004-2008).[16] According to Eurostat, as of 1 January 2009 there were 31.8 million foreigners living in the EU (6.4 per cent of the total population). Of these, 19.8 million are citizens of non-EU countries.[17] The illegal foreign resident population in the EU is estimated at 1.9 to 3.8 million in 2008. (2007). Some sources claim the number of irregular migrants is 2.8-6 million or even up to 8 million.[18] Over half of illegal immigrants entered the EU legally but became illegal due to overstay.[19] In 2010 540,000 illegal immigrants were apprehended in the EU but only 226 000 (around 40 per cent) of these were effectively removed. [20]

The European Union, with 500 million inhabitants, over 42,000 km of coastline, almost 9,000 km of land borders and approximately 1800 border crossing points sees every year around 700 million external border crossings. About a third of these border crossings are made by third country nationals who are checked at the crossing points at EU external borders. It is forecasted that border crossings will continue to rise significantly, especially at airports. According to Eurocontrol (European Organisation for the Safety of Air Navigation) the number of border crossings at airports will increase from 400 million in 2009 to 720 million in 2030.

This handful of statistical data shows challenges and problems posed by the growing mobility of persons. It is obvious that the flow of people and goods involves a number of risks and threats to the security of people, territory and infrastructure on the territory of EU Member States. It has directly to do with the control and management of immigration as well as prevention and combating of threats to EU security. This double-edged policy is not easy to be carried out in an integrated form. However, an integrated border management is a kind of solution to that dilemma, trying to link positive, inclusionary elements of EU

[16] See: Eurostat, Migrants in Europe. A statistical portrait of the first and second generation, 2011 edition, Luxembourg 2011, pp. 16-19.
[17] Europe in figures — Eurostat yearbook 2011, Luxembourg 2011, p. 150.
[18] Size and Development of Irregular Migration to the EU. CLANDESTINO Research Project, http://irregular-migration.net/typo3_upload/groups/31/4.Background_Information/4.2.Policy_Briefs_EN/ComparativePolicyBrief_SizeOfIrregularMigration_Clandestino_Nov09_2.pdf [accessed 23 February 2011]
[19] Commission Staff Working Document accompanying document to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Preparing the Next Steps in Border Management in the European Union. Summary of the Impact Assessment, doc. SEC(2008) 154, 13 February 2008, pp. 2-3.
[20] Communication from the Commission to the European Parliament and the Council - Smart borders - options and the way ahead, COM(2011) 680 final, Brussels, 25 October 2011, p. 4.

immigration policy, with negative, exclusionary components of EU internal security strategy. An integrated border management system is therefore a prospective remedy to shortcomings and limitations to EU comprehensive approach to migration and border control. The border management system is the key control mechanism for overall migration management. According to the European Commission, "the concept of an integrated border management involves combining control mechanisms and the use of tools based on the flows of persons towards and into the EU. It involves measures taken at the consulates of Member States in third countries, measures in cooperation with neighbouring third countries, measures at the border itself, and measures taken within the Schengen area."[21]

An important and telling aspect of an integrated border management project for the EU was its technological bias and stress on data collection and processing, information exchange, knowledge management and even intelligence sharing. The concept of the EU's integrated European Border Management Strategy, put forward under Finnish Presidency in 2006[22] was strongly linked to modern technologies and IT systems. An automated border control was identified with electronic surveillance, biometric identifiers and data exchange systems. The "border package" presented by the Commission on 13 February 2008 recommended establishing a new border surveillance system and setting up a new comprehensive framework for effective integrated border management (IBM) in the EU. This framework should include the four basic components:

- border control (checks, detection, monitoring and surveillance) including the necessary risk analysis and criminal intelligence;
- investigation of cross-border crime;
- a four-tier access control model (measures in third countries, cooperation with neighbouring countries, control measures within the area of free movement);
- cooperation between the authorities in the field of border management at the national and international level (border guards, customs and police authorities, security services and other relevant authorities);

[21] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Report on the evaluation and future development of the FRONTEX Agency. Statistical data. SEC(2008) 150, 13 February 2008, p. 3.

[22] Development of the EU's Integrated Management System for External Borders. Border Management Strategy, Informal JHA Ministerial Meeting, Tampere, 20-22 September 2006, http://www.statewatch.org/news/2006/sep/eu-jha-informal-borders.pdf [accessed 8 October 2006].

- coordination and coherence of action taken by the Member States along with institutions and agencies of the European Union.[23]

The institutional architecture of IBM combines existing EU border agencies with information systems and proposed control and surveillance solutions based on new technologies. The elements of this architecture are:

- Frontex (EU Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union),
- RABITs (Rapid Border Intervention Teams),
- EUROSUR (European Border Surveillance System),
- Control and surveillance systems (entry/exit, Registered Traveller Programme, electronic travel authorisation, Passenger Name Records),
- Large-scale information systems (Schengen Information System, Visa Information System, Eurodac).

Frontex was established by Council Regulation of 26 October 2004 with a view to improving the integrated management of the external borders of the EU's Member States. Its main tasks include coordination of operational cooperation between Member States in the field of management of external borders; assistance to the Member States on training of border guards; risk analyses and technical expertise in the control and surveillance of external borders; support for the Member States in circumstances requiring technical and operational assistance at external borders; assistance to the Member States in organizing joint return operations; information exchange and cooperation with appropriate EU agencies and international organizations.

Since the European Council in Brussels in October 2009 there has been a strong will among the Member States and a commitment on the part of the Commission to strengthen operational capabilities of Frontex and endow this agency with new tasks. The European Council called for the enhancement of Frontex and progress in its development on the basis of the preparation of common operational procedures for joint operations at sea, increased

[23] Council Conclusions on Integrated Border Management. 2768th JUSTICE and HOME AFFAIRS Council meeting, Brussels, 4-5 December 2006, http://eu2006.fi/NEWS_AND_DOCUMENTS/CONCLUSIONS/VKO49/EN_GB/1165226396565/_FILES/76364282267959390/DEFAULT/91978.PDF [accessed 8 December 2006].

operational cooperation between Frontex and countries of origin and transit of illegal migrants and prospective responsibility for and financing of joint return flights.[24] These proposals were partly taken into account in a regulation of 25 October 2011 amending the 2004 Frontex regulation.[25] The Agency will evaluate, approve and coordinate proposals for joint operations and pilot projects made by Member States. It may itself initiate and carry out joint operations and pilot projects in cooperation with the Member States concerned and in agreement with the host Member States. It may also decide to put its technical equipment at the disposal of Member States participating in the joint operations or pilot projects.

The new provisions allow for setting up European Border Guard Teams deployed during joint operations, pilot projects and rapid interventions. At the request of a Member State in urgent and exceptional cases related to high pressure at external borders of large numbers of third-country nationals trying to enter the territory of that Member State illegally, Frontex may deploy on the territory of the requesting Member State for a limited period one or more European Border Guard Teams.

Frontex will also provide the necessary assistance, finance or co-finance from its budget, and at the request of the participating Member States ensure the coordination or the organization of joint return operations, including through the chartering of aircraft for the purpose of such operations.

Rapid Border Intervention Teams (RABITs) may be set up on the grounds of the provisions of Regulation 863/2007 of 11 July 2007. Any Member State faced with a situation of 'urgent and exceptional pressure' of migrants at its external border may submit a request to organise a RABIT. Every Member State should contribute to the so-called Rapid Pool placing at the common disposal an appropriate number of border guards available for deployment at the request of Frontex. This agency would determine the composition of teams but the the profiles and the overall number of border guards belonging in the Rapid

[24] Brussels European Council 29/30 October 2009. Presidency Conclusions, doc.15265/1/09 REV 1, 1 December 2009.

[25] Regulation (EU) No 1168/2011 of the European Parliament and of the Council of 25 October 2011 amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, Official Journal of the European Union, L 304, 22 November 2011, p. 1.

Pool should be decided by the Management Board. For now RABITS were set up only on few occasions mostly for joint border exercises and training. The only case for a "mature" rapid border intervention was the crisis at Greek-Turkish Border in late 2010. At the request of the Greek government, a RABIT was deployed in the Greek-Turkish border for the period of four months (November 2010 – March 2011). 175 guest officers from 26 Member States assisted their Greek colleagues in controlling the border areas as well as in identifying the apprehended irregular immigrants.

EUROSUR (European Border Surveillance System) was outlined in the Communication from the Commission of 13 February 2008. The objective set in the proposal was the establishment of a single national coordination centre and a single national border surveillance system in each of the Member States located at the eastern land and the southern maritime external borders of the EU. It focused on enhancing border surveillance in order to reduce the number of illegal migrants, contribute to the prevention of cross-border crime, provide the common technical framework for cooperation and 24-hour communication between the competent authorities of the Member States. Moreover EUROSUR should help the Member States achieve situational awareness at their external borders, meaning the capability to detect cross-border movements and find reasoned grounds for control measures, as well as enhance the reaction capability of their law enforcement services, conceived of as a lapse of time required to control any cross-border movement and means necessary to react adequately to unusual circumstances. Lastly, EUROSUR should assist the Member States in acquiring integration capability that should allow establishing an integrated network of reporting and surveillance systems on external land and sea borders. EUROSUR is still in its conceptual phase, it should become operational in 2013.

The **entry/exit system** is a system that should apply to third country nationals admitted for a short stay (up to 3 months). The system should include the recording of information on the time and place of entry, the length of stay authorised, and the transmission of automated alerts directly to the competent authorities in case of 'overstaying'. The general objectives of the entry/exit system are to reduce illegal immigration (especially overstayers), contribute to the fight against terrorism and serious crime and improve the effective management of economic migration. This system could

become operational by 2015, following an effective and complete rollout of the Visa Information System.

The **Registered Traveller Programme** is a sort of an automated border control system enabling the automated verification of a traveller's identity without the intervention of border guards. It is thus intended to facilitate the crossing of EU external borders for bona fide travellers, while ensuring overall coherence of EU border policy. This programme is addressed primarily to third-country nationals who could present proof of sufficient means of subsistence, holding a biometric passport and – if necessary, the visa valid for limited period. Among prospective users of this programme one can also see EU citizens crossing the external borders.

The **entry/exit** system and **Registered Traveller Programme** could be combined as they are complementary, have impacts on the border checks at the external borders, and share a common approach to the practical border checks, information flows and management of resources. According to the Commission, 'these systems will cancel out each others´ effects as to the management of border check personnel and the average time required for border crossings.

Electronic System for Travel Authorisation (ESTA) is based on the assumption that a traveller wishing to enter a territory of any of the Member States would need to apply, via the internet, for an authorisation to travel based on common criteria. The Commission, in the 2011 Communication on smart borders, argued that the establishment of an EU ESTA for visa-exempted third-country nationals should be discarded as "the potential contribution to enhancing the security of the Member States would neither justify the collection of personal data at such a scale nor the financial cost and the impact on international relations." [26] The Commission pointed out that any EU ESTA would not be an alternative for an entry/exit system as it could not be used to monitor current flows at border crossings. Moreover, the Commission emphasized the rationale for an RTP exempting in principle registered travellers from the ESTA requirement.

[26] Communication from the Commission to the European Parliament and the Council - Smart borders - options and the way ahead, COM(2011) 680 final, Brussels, 25 October 2011, p.7.

However, the US homeland security authorities, regularly contacting their European counterparts, have stressed the effectiveness of their ESTA and called for reconsidering the rationale for an EU travel authorization system. Recently, the US Attorney General, Eric Holder, and the Secretary for Homeland Security, Janet Napolitano, attending the ministerial meeting of the G6 Group in Munich in May 2012 underlined that their Electronic System for Travel Authorisation had been a great success, enabling them to detect a number of potential terrorists seeking to travel to the United States.[27]

The **Passenger Name Record** (PNR) is a set of personal data and technical information on individual and group travels. PNR data are contained in database records of computer reservation systems registering travel movements, usually flights, and include personal passenger data, information on travel agent, schedule and itinerary and other relevant information. In the context of border management and security governance, the collection and analysis of PNR data should help the law enforcement authorities to identify high risk persons and other threats to air traffic. The extensive use of PNR data was observed in the aftermath of the 9/11attack as part of US counterterrorism policy (Adam 2006).

The European Union, initially hesitant to taking advantage of the PNR for counterterrorist purposes due to data protection standards, after the 2004 Madrid terror bombing subscribed to US position. In Declaration on combating terrorism, adopted by the European Council following the Madrid terrorist attack, the Commission was called upon to work out a proposal for a common EU approach to the use of PNR data for law enforcement purposes . The Commission was once more invited to bring forward such a proposal in the Hague Programme. Meanwhile agreements for the transmission of PNR data for travel by air were concluded between the EU and the United States, Canada and Australia.

Several months after the conclusion of the EU–US PNR Agreement, the European Commission put forward a proposal for a framework decision on the use of PNR for law enforcement purposes in the EU (so-called EU PNR proposal). The objective set out in the proposal was to grant the competent authorities of the Member States access to PNR data of passengers collected by air carriers in international flights. For the purpose of preventing and combating terrorist offences and organised crime, PNRs were subject to collection and

[27] Home Office, G6 meeting, Munich, 24th of May 2012, p. 3 [http://www.statewatch.org/news/2012/jun/eu-g6-munich-may-2012.pdf, accessed 11 June 2012].

retention by state authorities and to transfer and exchange between them. Sensitivity of data protection issue, potential risks to civil liberties and concerns for potential infringements of EU data protection regime expressed by the European Parliament, the Fundamental Rights Agency, teh European Court of Justice, European Data Protection Supervisor and numerous NGOs have delayed legislative works on the framework decision on EU PNR.

The above-described elements of EU integrated border management system have shown evidently the directions of rapid evolution and development of EU internal security policy in its territorial/physical dimension. The stress on physical identification of persons crossing the external borders or residing on the territory of Member States, the technologically biased management of identity of third-country nationals, and – last but not least – high-tech systems of border surveillance, perimeter control, automated targeting and risk-profiling reflects the commitment among EU institutions and agencies as well as the Member States to apply widely instruments of control and protection against potential risks and threats to EU internal security. In other words, IBM is unambiguously intended to securitize migrations and turn the external borders into automated gates.

EU 'smart borders' concept

A key element of digital borders is its interlocking into an integrated border management system. The European Union since 2006 has been decisively pushing the Member States for introducing and/or developing and reinforcing elements of such a system, especially implementing and enhancing 'e-borders' devices and solutions. The 2008 "border package" put forward by the Commission contained numerous proposals aiming to apply as wide as possible modern tools of control and surveillance, among them systems of automated verification of a traveller's identity and the recording of information on the length of authorized stay, and the transmission of automated alerts in case of overstaying. Due to certain political and human-rights reservation as well as technical and technological concerns, the implementation of the Commission's package was prolonging slowly and in some areas was stalled.

The breaking point, at least from the political point of view, was the European summit in June 2011 where, after "an extensive debate", the heads of states and government of EU Member States set orientations for the development of the EU's migration policy, the governance of the Schengen area and the control of external borders. The European Council decided that efforts should be taken to ensure that the external borders are effectively managed by "pushing forward rapidly with work on <<smart borders>>, to ensure that new technologies are harnessed to meet the challenges of border control. In particular, an entry/exit system and a registered travellers' programme should be introduced."[28]

The Commission, invited to present further ideas in that respect, issued in October 2011 the Communication "Smart borders - options and the way ahead".[29] According to the Commission the "smart borders" initiative should improve the management and control of travel flows at the external borders by reinforcing checks while speeding up crossings for regular travellers. Because there is no detailed description of the exact elements, functions or modalities of the concept of smart borders as a technical project, one should see it as a political design galvanized by the crisis of the Schengen area and growing anti-immigrant attitudes in several Member States.

The concept of smart borders has two components: an entry/exit system (EES) and a registered traveller programme (RTP). This means, paradoxically enough, that the Commission went back to its original 2008 proposal regardless of previous doubts concerning feasibility of linking those two components into a comprehensive technical and administrative arrangement. According to the Commission, an EES would allow the accurate and reliable calculation of authorized stay as well as the verification of the individual travel history for both visa holders and visa exempted travellers. It would do so by replacing the current system of stamping passports with an electronic registry of the dates and places of third country national admitted for short stays. A registered traveller programme is addressed to frequent travelers, especially to pre-vetted and prescreened third-country nationals. It should facilitate border crossings for *bona fide* travellers at the Schengen

[28] European Council 23/24 June 2011. Conclusions, doc. EUCO 23/11, Brussels, 24 June 2011, point 24 (p. 9).

[29] Communication from the Commission to the European Parliament and the Council - Smart borders - options and the way ahead, COM(2011) 680 final, Brussels, 25 October 2011.

external border, reduce the time spent at the crossing points and facilitate cross-border contacts. As far as possible, both systems would make use of new technologies such as Automated Border Control or Biometric Matching System for the purposes of visa policy.

As to technical/administrative matters, the Commission observed that setting up a RTP effectively depends on setting up an EES. There are also significant financial benefits (savings) if the two systems are built simultaneously, using similar infrastructure at the central level. The Commission advocated the creation of a central database and suggested that this could be combined with a token system for registered travellers. Each individual token would contain a unique identifier which would provide access to the central database. The two systems should be interoperable and centralized in order to avoid replication of traveller's data stored in a national system. These data should have at the beginning alphanumeric form and only at a later stage biometric data could be activated. However, the majority of the Member States, following discussion in the Council and at working groups, wished to introduce biometrics into the EES from the outset.[30] The newly established European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, which is due to start operations at the end of 2012, would be responsible for the development and operational management of the systems.

Regarding practical implementation of both projects, the Commission set substantive and procedural principles to serve as a benchmark in this area. These principles include: (1) respect for fundamental rights, in particular the right to privacy and data protection; (2) necessity; (3) subsidiarity; (4) accurate risk management; (5) cost-effectiveness; (6) bottom-up policy design; (7) clear allocation of responsibilities; (8) review and sunset clauses. Apart from fundamental rights, which in themselves present a politically and legally sensitive issue, the most relevant principle is necessity. It should not only legitimize in practical terms the project of smart borders but it also could deliver a rationale for further progress and development of the border management system in the EU. This is why the Commission clearly stated that – due to the lack of reliable information on overstayers from the Member States - it would be difficult to predict how many persons should actually be apprehended as

[30] See: Communication from the Commission to the European Parliament and the Council: "Smart borders - options and the way ahead" - Summary of discussions, doc. 17706/11 LIMITE, Brussels, 29 November 2011, p. 2; EU Conference on Innovation Border Management, Copenhagen, 2-3 February 2012, doc. 7166/12, Brussels, 2 March 2012.

a result. The existing IT systems collecting information on third-country nationals, namely the SIS and VIS, should be of some assistance. To alleviate any allegations of inadequacy and arbitrariness, the Commission underlined that the entry/exit system should bring benefits not only for the Member States, but it should also modify the existing framework of the Partnership for Migration, Mobility and Security with certain neighbouring countries through a better and more accurate assessment of current visa policies and visa facilitation regarding respective third countries.

While in the case of an EES the Commission highlighted the limits and possible shortcomings of this system on the basis of early assessment and evaluation of the existing prerequisites, a RTP was treated in a different, proactive manner. In the Commission's view accurate risk management and pre-screening are critical features of the whole mechanism justifying the adequacy of technical solutions and total costs of the system.

Conclusions

EU border management is to a significant degree, at least in its 'negative' aspect of preventing illegal entry to the EU and expelling irregular migrants from the EU, a sheer example of mechanisms of selective differentiation driven by the logic of insecurity. Physical differentiation, taking the form of visa policy, passport controls, travelers registry, separate lanes in border crossing points and remote digital screening, is the dominant feature of what Hooper defined as borderwork.[31] It is driven by the performance of specific power relations seeking to produce and reproduce a bounded identity. Borderwork thus depends largely on technical tools and their practical usefulness subject to technological advancement and quality of performance. In this respect biometrics emerged as a high-tech practical solution to the growing problem of management of identity of persons incoming to the EU.[32] It is no wonder that the Member States are keen on introducing biometric identifiers and connect

[31] B. Hooper, Ontologizing the borders of Europe, in: O. Kramsch, B. Hooper (eds.), *Cross-Border Governance in the European Union,* London and New York: Routledge, 2004, p. 218; N. Vaughan-Williams, Borderwork beyond Inside/Outside? Frontex, the Citizen–Detective and the War on Terror, *Space and Polity*, 2008, 12 (1), pp. 63–79.

[32] J. *Ashbourn*, *Practical Biometrics: From Aspiration to Implementation*, Berlin: Springer Verlag, *2004, p. 1; A.* Ceyhan, Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics. *Surveillance & Society,* 2008, 5 (2), p. 113; D. Day, Biometric Applications, Overview, in: S.Z. Li, A.K. Jain (eds.), *Encyclopedia of Biometrics*, New York: Springer Science+Business Media, 2009, pp. 76-79.

them with a Biometric Matching System. Applied to asylum, immigration, visa and border control policies of the EU, biometric identification and authentication of foreigners became a powerful method of securitization policies.

The project of EU smart borders is a typical example of "virtual fencing" which – as many examples in the past have proved – carries with itself numerous challenges, dilemmas and flaws. First, the concept of smart borders is exclusionary in a sense that it stems from a reactionary, defensive attitude towards "aliens", often consists in identifying threats and risks and labeling it a security problem or dilemma which requires application of certain political, organizational and technical solutions in order to "maintain stability" or "protect public sphere". It encompasses various roles performed by police, intelligence, border guards or visa administration, involving criminal profiling, surveillance of public space, detailed checks on border crossing points, monitoring of borders, prevention and countering cross-border organized crime, illegal migration, financial crime, the use of forged or false documents, or even visa blacklisting.

Second, its feasibility is highly questionable given the number of persons crossing external borders of the EU, the amount of data for storing in databases, an average time needed to perform reliable verification of a foreigner's identity, the reliability of tokens etc. Moreover, new systems (EES and RTP) have to be somehow connected to the existing (VIS) and in the making (SIS II) large IT systems collecting and storing centrally data referring to the crossing of external borders of the EU. In an opinion on the communication of the Commission on migration issued in July 2011 by the European Data Protection Supervisor (EDPS) emphasis was placed on the need to assess the use of existing systems and to prove the necessity for an entry/exit system in particular.[33] Actually, the Commission in the communication on smart borders acknowledged that "a fully operational and developed VIS is a prerequisite for the implementation of a Smart Borders system." Hence, it seems that the smart borders concept for now has "overloaded" the existing institutional and technical architecture with respect to border management and information processing.

Third, possible legal implications of "hits" in the system raise further doubts. Ben Hayes and Mathias Vermeulen, authors of an assessment of the costs of EU border

[33] Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on migration, Official Journal of the European Union, C 34, 8 February 2012, p. 18.

surveillance initiatives and its impact on fundamental rights argue that "An overstayers alert can only ever constitute a *presumption* of illegal residence, and stringent follow-up controls with regard to the treatment of people identified as such will be needed to ensure that the EU respects its human rights obligations. An administrative procedure must be completed in order to determine whether the person has the right to stay legally in EU territory, and this procedure must give the traveler the chance to explain the circumstances of any overstay."[34]

Fourth, the project has a clearly preventive objective, aiming to detect, identify and quantify overstayers in the case of EES and support the efforts to prevent and combat illegal immigration and cross-border crime in the case of RTP. Given that, its preventive value will be still questionable with regard to illegal migration and people smuggling. It is indeed focused on legal migrants who prolong their stay in the EU yet this is only a part of the problem. One could even expect a temporary or long-term intensification of illegal crossings at external borders, especially done by organized criminal organizations dealing with trafficking in human beings.

The project of smart borders does not respond clearly to the requirements of a comprehensive, integrated management at EU external borders. An "electronic fencing" system and IT solutions seem to be loosely connected to the institutional and operational framework of EU border policy. In terms of EU security strategy, its impact will be rather low if data flow is based on alphanumeric format and considerably higher if biometric identifiers are required. Smart borders as any mechanical tool for control and surveillance can contribute to risk analysis, threat assessment and situational awareness at EU external borders but hardly can be accepted as a system facilitating border crossings and enhancing cross-border cooperation with third countries.

[34] B. Hayes, M. Vermeulen, Borderline. EU Border Surveillance Initiatives. An Assessment of the Costs and Its Impact on Fundamental Rights, Berlin, May 2012, p. 72 [http://www.boell.de/downloads/DRV_120523_BORDERLINE_-_Border_Surveillance.pdf, accessed on 2 June 2012]